UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/783,843 | 02/15/2001 | James Alexander Reeds III | 1999-0274 | 2575 |

7590 05/02/2005

Charles A Mirho
112 W 37th St
Vancouver, WA 98660

| EXAMINER | |
|---|---|
| DINH, MINH | |
| **ART UNIT** | **PAPER NUMBER** |
| 2132 | |

DATE MAILED: 05/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

| Office Action Summary | Application No. | Applicant(s) |
|---|---|---|
| | 09/783,843 | REEDS ET AL. |
| | Examiner | Art Unit |
| | Minh Dinh | 2132 |

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *14 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *29-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *29-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 February 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____

U.S. Patent and Trademark Office

PTOL-326 (Rev. 1-04) **Office Action Summary** Part of Paper No./Mail Date 20050427

## DETAILED ACTION

### *Response to Amendment*

1. This action is in response to the amendment filed 01/14/2005. Claims 1-28 have been canceled; claims 29-36 have been added.

### *Response to Arguments*

2. Applicant's arguments filed 01/14/2005 have been fully considered but they are not persuasive. Applicant argues that Lockhart does not teach the comparison of checksums for the purpose of detecting loss of stream cipher synchronization (page 4, 2nd paragraph). Lockhart teaches comparing reference values that are checksums of transmitted data packets to detect loss of cipher synchronization (fig. 2; col. 4, lines 54-66; col. 2, lines 25-31). Regarding applicant's arguments that Lockhart would not anticipated the present claims and that Lockhart's teaching wastes bandwidth and requires additional information to be transmitted with the encrypted payload (page 5, 2nd par.), applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. Applicant argues that none of the references teaches detecting the loss of cipher synchronization at a layer other than the layer that provides cryptography. It is established in the previous Office action that checksums are used to detect loss of cipher synchronization and that checksum calculation and comparisons is performed at the network layer which is different from sub-network layer that provides cryptography.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 29-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lockhart et al. (5,841,873) in view of Ahmed et al. (6,747,961) and Menezes et al. ("Handbook of Applied Cryptography").

Regarding claim 29, Lockhart discloses a method comprising: decrypting an encrypted data packet to produce a decrypted data packet (fig. 2, step 215); calculating a calculated checksum for the decrypted data packet (fig. 2, step 221; col. 4, lines 54-66; col. 5, lines 46-65); comparing a checksum extracted from the decrypted data packet with the calculated checksum (fig. 2, step 221); and detecting a loss of cipher synchronization if the calculated checksum does not match the checksum extracted from the decrypted data packet (fig. 2, step 300; col. 2, lines 25-31).

Lockhart does not disclose a security sub-network layer performing decryption. Ahmed discloses a security sub-network layer located below a network layer and above the MAC layer, the security sub-network layer providing encryption/decryption function to a network layer (col. 3, lines 53-59; fig. 3B). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the security sub-network layer of Ahmed into the method of Lockhart, the sub-network layer

providing encryption/decryption function to a network layer. Such a sub-network protocol layer provides the communication systems with various mobility management functions (col. 3, lines 59-63).

Lockhart does not disclose that the encryption algorithm is a stream cipher. Menezes discloses using stream ciphers (p. 161, see 6.1 Introduction). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Lockhart to use a stream cipher, as taught by Menezes, because stream ciphers are advantageous in situations where transmission errors are highly probable.

Regarding claims 30-34, Lockhart does not disclose calculating the calculated checksum at a network layer. However, Examiner takes Official Notice that using Transmission Control Protocol (TCP), which is part of a network layer (specification page 6, lines 22-24), to determine the integrity of a transmitted payload is well known in the art. In particular, the transmitting TCP calculates a checksum based on the payload data to be transmitted and includes the checksum in the TCP header for transmission; the receiving TCP then performs the same calculation on the payload data received and compares the result with the received checksum; a discrepancy indicates some error. It would have been obvious at the time of the invention was made to one of ordinary skill in the art to calculate the calculated checksum at a network layer since Examiner takes Official Notice that using TCP to determine the integrity of a transmitted payload data is well known in the art. Since Lockhart teaches comparing the checksums to detect the loss of cipher synchronization, it would be obvious to use the network layer, which

compares the checksums to detect errors, to detect the loss of cipher synchronization. Accordingly, the checksums are for a network layer data payload and that the extracted checksum is extracted from the network layer header.

Regarding claim 35, Lockhart further discloses resetting a lower layer if the calculated checksum does not match the checksum extracted from the decrypted data packet (fig. 3, step 317), resetting a lower layer meets the limitation of re-synchronization.

Regarding claim 36, please refer to the discussion of using TCP to determine the integrity of a transmitted payload data above.

***Conclusion***

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dinh whose telephone number is 571-272-3802. The examiner can normally be reached on Mon-Fri: 10:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MD
Minh Dinh
Examiner
Art Unit 2132

MD
4/27/05

Gilberto Barron
GILBERTO BARRON Sr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

**CERTIFICATE OF FACSIMILE TRANSMISSION**

**for**

Attorney Docket Number: FSP0053
Client Reference Number: AWS 742.US
Title: DETECTING A LOSS OF KEY STREAM SYNCHRONIZATION IN A COMMUNICATION SYSTEM
Application Number: 09/783,843
Filing Date: Thursday, February 15, 2001
First Named Inventor: Reeds III, James A.
Group Art Unit: 2132
Examiner Name: Dinh, Minh

---

I hereby certify that the following is being transmitted via facsimile to telephone number 571-273-8300 on Monday, August 01, 2005.

Signature:
Printed name: Charles A. Mirho

Contents of This Correspondence

---

5 pages of amendment and reply to office action
1 page of Certificate of facsimile
1 page of Request for continued examination
1 page of Fee transmittal to PTO

Authorization to debit deposit account for $790 dollars.